Privacy notice / fact sheet / consent form for staff employed / engaged to work at Cantrell Primary School

General Data Protection Regulation (GDPR)

The following information is designed to ensure you are familiar with the General Data Protection Regulation (GDPR) which came into effect on 25 May 2018 and tell you how we as a school collect and use your personal data

Cantrell Primary School aims to ensure that personal information is treated in a lawful, fair and transparent manner. Cantrell Primary School is the data controller of personal information. i.e the school determines the purposes for which, and the manner in which, any personal data relating to staff is to be processed. However, Cantrell Primary School, and therefore any person who handles personal data on behalf of the school, fully endorses and adheres to the data protection principles set out in Article 5 of the GDPR and sections 83-89 DPA 2018 and shall be responsible for and be able to demonstrate compliance with the six data principles outlined below:

The Six Data Protection Principles
Personal Information shall be: 1. processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency) 2. collected for specified explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;(purpose limitation) 3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;(data minimisation) 4. accurate and where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy) 5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject (storage limitation) 6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality)

Useful definitions
Personal data - any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. **Personal data breach -** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to personal data transmitted, stored or otherwise processed.

Consent - any freely given, specific, informed and unambiguous indication of wishes, by a statement or clear affirmative action which signifies agreement to the processing of data.
Special categories of personal data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural persons sex life or sexual orientation.
Data subject - the person identified by the information that we collect the data from and about. The individual teacher is the data subject.
Data controller - an organisation or body that is responsible for complying with Data Protection Law determines the purpose and means of processing the personal data.
Processing - includes any operation or set of operations, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, use, disclosure, erasure or destruction.
Subject Access Request - right to access personal data by the parent/carer of the pupil.
DPO - Data Protection Officer

Fundamental to the management of data is the role of Data Protection Officer. **Jill Weedop is our School Data Protection Officer.** The DPO's role is to oversee and monitor the school's Data Protection procedures and to ensure they are compliant with GDPR.

The DPO will have the following tasks:

- Informing and advising school of their obligations under GDPR – be involved, properly and in a timely manner in all issues that relate to the protection of personal data
- Monitoring compliance with GDPR-annual audit
- Awareness raising and training of staff-annually
- Reporting to management
- Co-operating with the ICO
- Remaining aware of the risks associated with processing of personal data
- Communicating with children / parents / carers as appropriate

The DPO can be contacted on dpo@cantrell.nottingham.sch.uk

Data we collect and hold at Cantrell Primary School

- Personal information e.g. name, gender, date of birth, address, national insurance, contact details (telephone and email) / contract of employment / all details required to administer payroll / remuneration details / NI and pension details / bank details / car registration details
- Characteristics e.g. ethnicity, language, nationality, country of birth, equality information
- Interview application forms / references / Curriculum Vitae / accreditations and certificates
- SCR / DBS / vetting information / Right to work in the UK (safeguarding compliance)
- Medical information including accident / incident information / Occupational Health referrals and sickness notes
- Attendance Information
- Appraisal documentation
- Record of training and CPD
- SEN/D information (where appropriate)
- Photographs with consent (for use on the school website, newsletter, school noticeboard, personnel folder in line with the consent form attached to this document)
- Grievances /complaints / disciplinaries
- Minutes of meetings to include senior team, staff, multi-agency

Why does Cantrell Primary School need your data and personal information?
Processing data and personal information.
Employee rights.

We will, when processing personal information about any individual:

- Observe fully the conditions regarding the collection and use of information and meet the school's legal obligations under the GDPR and the Data Protection Act 2018
- Collect and process appropriate information only to the extent that it is needed to enable the school to perform its duties and services and fulfil operational needs.

Purposes will include the following:

1. Providing education and pastoral care
2. Providing activities for pupils including school trips and after school clubs and activities
3. Safeguarding and promoting the welfare of children
4. Providing references for pupils and staff
5. Providing human resources function for staff
6. Ancillary purposes to education including completing contractual obligation

- Collect and process information to comply with any legal requirement;
  e.g. We are required to share information about our staff with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments and when required, with the Local Authority human resources team including payroll and occupational health.
  e.g. Where the information is required by the police for the prevention and detection of crime.
  e.g. Where a relevant Information Sharing Agreement is in place e.g. SIMS (our Management Information System provider).

We will ensure that the individual about whom information is held can exercise their rights under the Act unless an exemption applies.

Employees can exercise the following rights;

- to be informed that processing is being undertaken
- to prevent processing in certain circumstances
- to correct, rectify, block or erase information, which is regarded as incorrect information
- of access to personal information
- to erasure
- to portability where applicable.

NB.

1. *Personal Information will only be disclosed to persons (internal and external) where their authority to receive it has been explicitly established.*
2. *Where the processing of your data is based on explicit consent, you have the right to withdraw this consent at any time.*

Retention schedule

Information processed will not be excessive or irrelevant to the notified purposes.
Information will only be held/retained for so long as is necessary for the notified purposes, after which it will be deleted or destroyed.

The school has published a 'retention schedule' in line with LA guidance-which can be found on the staff share drive. Whenever information is processed, we will always endeavour to ensure that it is up to date and accurate.

Data Incident Reporting / Data Breach
A data breach can be defined as a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so. Cantrell Primary School staff members must notify the Data Protection Officer/ Head Teacher directly by phone on 0115 9155770 or by e-mail on; dpo@cantrell.nottingham.sch.uk / headteacher@cantrell.nottingham.sch.uk / jacquie.ellis@cantrell.nottingham.sch.uk of any potential data incidents as soon as the incident occurs and in any event within 24 consecutive hours after occurrence. **It is important you receive acknowledgement of your email within 24 hours from one of the above email accounts, particularly during school holiday times.** Any reported data incident will be investigated appropriately and actions taken as necessary. Personal data breaches will be notified to the Information Commissioner's Office within 72 hours of the incident. All staff members must follow the school's Data Incidents and Breaches policy and procedure held on the staff sharedrive. If you have a concern about the way our school is collecting or using your personal data you can raise a concern with the school DPO or the Information Commissioner's Office (ICO). This can be done by telephone 0303 123 1113 Monday – Friday 9am – 5pm or e-mail registration@ico.org.uk

Supporting policies that can be found on the school staff share-drive include;
• Data Protection policy • Data Incidents and Breach Policy • FOI policy • Email Policy • Mobile Computing policy • IT Acceptable Use policy • Retention schedule

I can confirm I read the above information and have familiarised myself with the supporting school policies.

Name_____

Signed_____

Date_____

Staff consent form

To comply with the GDPR 2017/18 and the Data Protection Act 2018, Cantrell Primary School will need permission before we can photograph or make any recordings of you.

Sometimes school staff may appear on photographs and videos during the school year. We may want to use the images in printed publications, displays and even on our website. We may also make video recordings. We may also send images to the news media, or our school may be visited by the media who will take their own photographs or film footage (for example, of a visiting dignitary or other high profile event). Staff will often appear in these images. The news media may use the images in printed publications (including local or national newspapers), on televised news programmes or on their website. They then store them in their archive. They may also syndicate the photos to other media for possible use, either in printed publications, on websites, or both. When we submit photographs and information to the media, we have no control on when, where, if or how they will be used.

Please tick all the boxes that apply to you:

I give permission for my image to be taken for the purpose of providing a record of time at the school, e.g. in a class, a year photograph, a school team photograph, etc.	☐
I give permission for my image to be taken and used on displays, notices, etc. within the school which are generally only viewed by school staff and other visitors and pupils.	☐
I give permission for my image to be taken and used in publicity material for the school, including printed and electronic publications and video recordings.	☐
I give permission for my image to be used on websites and by the news media in printed and/or electronic form and stored in their archives. This might include images sent to the news media by the school and images / footage the media may take themselves if invited to the school to cover an event.	☐

We also need to your consent to forward email information from third parties e.g. SCENE, National Literacy Trust, Trade Unions that are related to school business or your own professional development.

I consent to receiving emails from 3rd parties that are related to school business.	☐

I have read and understood the information above.

Name: _____

Signed: _____

Date: _____

Data protection staff training slides-May 2018

Data Protection Law:

Introduction to the new General Data Protection Regulation and the Data Protection Act 2018

P A Fielding / C Hill
9th May 2018

The General Data Protection Regulation GDPR

- Comes into force on the 25 May 2018
- Data Protection Act 1998 will be repealed
- General Data Protection Regulation is also supplemented by the new Data Protection Act 2018

Summary of key changes to the Data Protection law by the GDPR

- More rights for the data subjects/pupils/employees/parents
- Increased penalties
- Mandatory Data Protection Officer for Haydn School
- Introduces the concept of privacy by design - Privacy impact Assessment mandatory in some cases
- Personal data breaches must be reported to the ICO in 72 hours
- Schools must keep records of processing
- Increased accountability

The General Data protection regulation and the Data protection Act 2018- key terminology

•Data subject
- The person identified by the information

•Data controller
- An organisation or body that is responsible for complying with Data Protection Law
- Determines the purpose and means of processing the personal data

•Processing
- Handling, storing, sharing or manipulating personal data

•DPO
- Data Protection Officer

To be compliant we must appoint a Data Protection officer (DPO)

DPO shall have following tasks:

- To inform and advise school of their obligations under GDPR – be involved, properly and in a timely manner in all issues that relate to the protection of personal data
- To monitor compliance with GDPR-annual audit
- Awareness raising and training of staff-annually
- Reporting to management
- Co-operating with ICO
- Think about risks associated with processing of personal data
- Communicate with children / parents / carers

School Policies and Guidance

- Data Protection policy
- Data Incidents and Breach Policy
- FOI policy
- Email Policy
- Mobile Computing policy
- IT Acceptable Use policy
- Records Management policy / retention schedule
- Data Flow Map
- Redaction Guidance

For clarification - definition of personal data

•Personal Data:

•Means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of Consent

•Consent: of the data subject means any freely given, specific, informed and unambiguous indication of the data subjects wishes by which he or she, by a statement or **by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her.

GDPR Consent

7 Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes

- Our consent forms will need reviewing
- No pre-ticked boxes
- **Must opt in not opt out**
- Granular consent

GDPR – Privacy notices

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

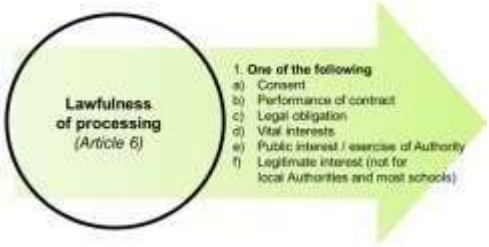
We will publish our Privacy Notice on the internet.

The Six Principles of Data Protection

In order to use personal data you must satisfy one of the following conditions;

1. Lawfulness, fairness and transparency
2. Purpose limitation-specific, explicit, legitimate purposes
3. Data minimisation-adequate, relevant, limited
4. Accuracy
5. Storage limitation - Retention
6. Integrity and confidentiality-Security

GDPR Purpose of Processing



When can special personal data be used?

Special personal data will only be processed fairly and lawfully as required by the first data protection principle if at least one of a number of **additional** conditions is satisfied (found in Article 9), which include the following:

- The individual has given his **explicit** consent to the processing of those personal data for one or more specified purposes
- The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security and social protection law
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- The processing relates to information which are manifestly made public by the data subject

When can provisions of the GDPR be exempted?

•Personal data can be exempted from the duty to process information fairly and lawfully to the extent necessary for making a disclosure, if an exemption applies:

CRIME PREVENTION EXEMPTION - Schedule 2, Part 1, Paragraph 2 (used to be S.29 DPA 1998) - Crime prevention / apprehension or prosecution of offenders / tax duty, or similar imposition

IMMIGRATION EXEMPTION - Schedule 2, Part 1, Paragraph 4 (new exemption) –

The maintenance of effective immigration control and the investigation or detection of activities that would undermine the maintenance of effective immigration control

LEGAL PROCEEDINGS/COURT ORDERS - Schedule 2, Part 1, Paragraph 5 (used to be S.35 DPA 1998) - Information required to be disclosed by law etc. or in connection with legal proceedings

There are others exemptions relating such as exam scripts and exam marks, confidential references and management forecasts.

Processors - Article 28

•Using system providers for processing your pupil data, using shredding companies to shred confidential paper waste, using cloud IT providers:

•GDPR makes clear that the school should only use processors that provide sufficient guarantees to implement appropriate technical and organisational measures to ensure the rights of the data subject and to be compliant with the GDPR

Increased enforcement powers

- New fines will be imposed on a two tier basis
- For contraventions such as record keeping and data processor contracts, failure to notify breaches within 72 hours a fine of 2% of turnover or 10 million Euros
- For contraventions of data protection principles, data subject rights the fine will be up to 4% of annual turnover or 20 million Euros
- Criminal offences

Incident to data breach

A situation or incident that results in, or has the potential to result in, a breach of one or more of the data protection principles.

- E.g. unlawful processing, inaccurate data, lack of security

GDPR Data Breaches - ICO school examples

- Website security - personal data accessible
- Insufficient pen testing, inaccurate coding
- Sending SPD via unprotected email
- Lost unprotected USB sticks including pupil data (academic progress)
- Unencrypted drives / laptops / devices stolen from staff homes / cars / bags
- School website hacked, administrator passwords stolen. One teacher used the same password for their website administrator access and their access to the main school pupil database
- Hackers accessed information from the database
- Spreadsheet uploaded to website - full details of pupil premium spending
- Technical measures - passwords
- Parent passwords to access child information not sufficiently strong

GDPR Individual rights

- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restriction of processing
- Right to data portability (Where consent gateway used)
- Right to object

Practical steps we will take to prevent a breach

- [illegible]
- Do not share passwords, use shortcode passwords or sign into systems for others
- Use the screen lock function
- Check the security on your smartphone if you receive school emails MDD
- Enable PC screen lock activation within 5 minutes
- Do not leave sensitive information on whiteboards when it is to be seen by 3rd parties e.g. parents evening lists
- All holder access / password access to computers
- Disable the memory access on the USB ports for accessing school data remotely
- Sensitive material will be locked in a cabinet or a locked room
- Keep the amount of information transported to a minimum
- Do not leave files in a car even when locked unless fitted with a safe
- Never use an unencrypted device – USB, laptop or phone
- Only use an encrypted email for example Cryptshare to transmit special personal information
- Only dispose of personal information by shredding
- Ensure that retention and disposal is considered and acted upon

Next Steps

- Publish privacy notice
- Construct and distribute consent forms
- Clarify Information Sharing Agreements
- Put data breach procedure in place to be able to report to the ICO in 72 hours
- Collect records of processing
- Carry out Privacy Impact Assessments
- Clarify encryption/password/security options
- Agree policy set
- Allocate secure document storage
- Ensure secure transportation of documents
- Regular device audits-if in doubt-ask
- Training for MDS / Cleaning staff / catering staff